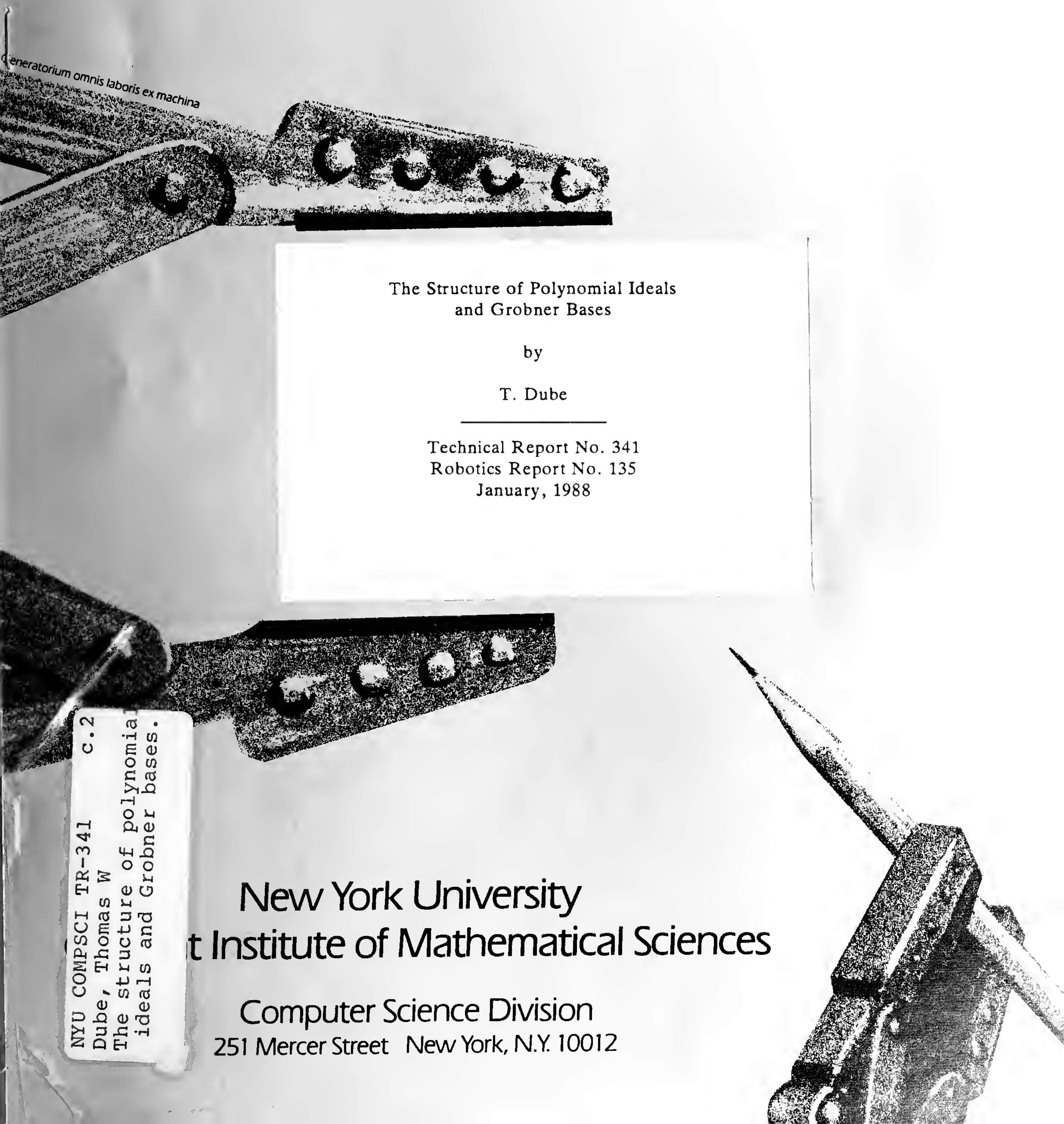
Robotics Research Technical Report



The Structure of Polynomial Ideals and Grobner Bases

by

T. Dube

Technical Report No. 341
Robotics Report No. 135
January, 1988

New York University
t Institute of Mathematical Sciences

Computer Science Division
251 Mercer Street New York, N.Y. 10012

The Structure of Polynomial Ideals and Grobner Bases

by

T. Dube

Technical Report No. 341
Robotics Report No. 135
January, 1988

New York University
Dept. of Computer Science
Courant Institute of Mathematical Sciences
251 Mercer Street
New York, New York 10012

Work supported in part by NSF grants #DCR-84-01898 and #DCR-84-01633.

The Structure of Polynomial Ideals and Gröbner Bases

Thomas W. Dubé [1]

Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, NY 10012.

January 5, 1988

Abstract

The use of Gröbner Bases is becoming increasingly important in algebraic computational geometry. As a result, there has been much activity in the recent years concerning the complexity of Buchberger's algorithm, and the degree of polynomials which it may produce. Bayer's thesis in 1982 provided the direction for recent research, and several recent papers have combined to show that the complexity of computing a Gröbner Basis for a given ideal is double exponential in the number of variables. This paper introduces a new partitioning of a polynomial ideal. Using this partitioning, the sharpened degree bound can be obtained using only combinatorial arguments, and without the need to change coordinate systems.

[1] Supported in part by NSF grants #DCR-84-01898 and #DCR-84-01633.

1 Reductions and Gröbner Bases

The definitions quoted here for Gröbner bases are based upon the writings of Bruno Buchberger. The properties of normal forms which are cited in this section are also results of his work. Gröbner bases are special bases for polynomial ideals with several important computational properties such as the ability to rapidly determine ideal membership. Grõbnerbases differ only slightly from the *standard bases* defined by Hironaka, and many of these concepts can be traced back to the work of Macaulay.

A total ordering $\underset{A}{<}$ on the power products of $\mathrm{PP}[X] = \mathrm{PP}[x_1, \ldots, x_n]$ is called an *admissible ordering* if the following two axioms are satisfied.

1. For all $x_i \in X$, $1\underset{A}{<}x_i$.
2. For all $a, b, c \in \mathrm{PP}[X]$, $a\underset{A}{<}b$ implies $ac\underset{A}{<}bc$.

Let h be a polynomial of $K[X]$ where K is an arbitrary field. For any fixed admissible ordering $\underset{A}{<}$, the $\underset{A}{<}$-least monomial of h is called the *head monomial of h with respect to $\underset{A}{<}$* and is denoted by $\mathrm{Head}_A(h)$. If the ordering is understood, then we may drop the subscript and denote the head monomial as simply $\mathrm{Head}(h)$. For I an ideal of $K[X]$, $\mathrm{Head}_A(I)$ will be used to denote the monomial ideal generated by $\{\mathrm{Head}_A(h) : h \in I\}$.

Let $F \subset K[X]$ be a set of polynomials, and $\underset{A}{<}$ a fixed admissible ordering. A polynomial h is then said to be F-reducible, if there exists $f_i \in F$, and $c \in K[X]$ such that $\mathrm{Head}_A(cf_i)$ is a monomial of h. The polynomial $g = h - cf_i$ is then called a reduct of h, and this relationship is denoted as $h \xrightarrow{F} g$. The transitive closure of the reduction operation $h \underset{*}{\xrightarrow{F}} g$ is defined to mean that there exists a series of polynomials $p_1, \ldots, p_k$ such that $p_1 = h$, $p_k = g$, and for all $i < k$, $p_i \xrightarrow{F} p_{i+1}$. Finally, g is called an F-normal form of h if $h \underset{*}{\xrightarrow{F}} g$, and g is not F-reducible.

Definition: A basis G is called a *Grõbner basis* of I with respect to $\underset{A}{<}$ if $\mathrm{Head}_A(I)$ is generated by the set $\{\mathrm{Head}_A(g) : g \in G\}$.

It is easy to verify that the following conditions are all equivalent.

1. G is a Gröbner basis for I with respect to $\underset{A}{<}$.

2. $G \subset I$ and for every $h \in I$ there exists a $g \in G$ such that $\mathrm{Head}_A(g)$ divides $\mathrm{Head}_A(h)$.

3. For all $h \in K[X]$, 0 is a G-normal form of h if and only if $h \in I$.

4. G is a basis for I and every $h \in K[X]$ has a unique G-normal form which may be denoted as $\mathrm{nf}_G(h)$.

It is also easy to verify that if F is a monomial basis for a monomial ideal I, then F is a Gröbner basis for I with respect to every admissible ordering.

The following lemmas provide some useful properties of normal forms.

Lemma 1 *Let G be a Gröbner basis for I with respect to $\underset{A}{<}$. Then for all $h \in K[X]$, $h - \mathrm{nf}_G(h) \in I$.*

Proof. This is a trivial consequence of the reduction algorithm.
Q.E.D.

Lemma 2 *Let G be a Gröbner basis for I with respect to $\underset{A}{<}$, Then for any $s, t \in K[X]$, $\mathrm{nf}_G(\mathrm{nf}_G(s) + \mathrm{nf}_G(t)) = \mathrm{nf}_G(s) + \mathrm{nf}_G(t)$.*

Proof. $\mathrm{nf}_G(s)$ and $\mathrm{nf}_G(t)$ consists entirely of monomials *not* in $\mathrm{Head}_A(I)$. Therefore,$\mathrm{nf}_G(s)+\mathrm{nf}_G(t)$ consists of monomials not in $\mathrm{Head}_A(I)$, and hence is a normal form itself.
Q.E.D.

Lemma 3 *Let G be a Gröbner basis for I with respect to $\underset{A}{<}$, then for any $s, t \in K[x]$,*

$$\mathrm{nf}_G(s + t) \;=\; \mathrm{nf}_G(s) + \mathrm{nf}_G(t) \;.$$

Proof.

$$\begin{aligned}
s + t - (s + t) = 0 \;&\Longrightarrow\; s + t - (s + t) \in I \\
&\Longrightarrow\; \mathrm{nf}_G(s) + \mathrm{nf}_G(t) - \mathrm{nf}_G(s + t) \in I \\
&\Longrightarrow\; \mathrm{nf}_G(\mathrm{nf}_G(s) + \mathrm{nf}_G(t) - \mathrm{nf}_G(s + t)) = 0 \\
&\Longrightarrow\; \mathrm{nf}_G(s) + \mathrm{nf}_G(t) - \mathrm{nf}_G(s + t) = 0
\end{aligned}$$

Q.E.D.

Corollary 1 *Let G be a Gröbner basis for I with respect to $\underset{A}{<}$, and let h_1 and h_2 be polynomials such that $h_1 - h_2 \in I$. Then* $\mathrm{nf}_G(h_1) = \mathrm{nf}_G(h_2)$.

From this corollary it can be seen that the set $\{\mathrm{nf}_G(h) \ : \ h \in K[X]\}$ is isomorphic to the quotient ring $K[X]/I$. We would sometimes like to consider sets of this type, in which we don't really care which Gröbner basis G is being used to define the normal forms. In a slight abuse of notation $K[X]/I$ will be used to denote $\{\mathrm{nf}_G(h) \ : \ h \in K[X]\}$ where G is some arbitrary Gröbner basis for I.

The following lemma has two very important corollaries.

Lemma 4 *Let G_1 be a Gröbner basis for I_1 with respect to $\underset{A}{<}$, and let G_2 be a Gröbner basis for I_2 with respect to $\underset{B}{<}$, where $Head_B(I_2) = Head_A(I_1)$. Then for any $h \in K[X]$,* $\mathrm{nf}_{G_2}(\mathrm{nf}_{G_1}(h)) = \mathrm{nf}_{G_1}(h)$.

Proof. Once again, a G_1-normal form consists of monomials which are not in $\mathrm{Head}_A(I_1)$, and hence are not in $\mathrm{Head}_B(I_2)$. This is therefore also a G_2-normal form.
Q.E.D.

Corollary 2 *Let G_1 and G_2 be Gröbner bases for the same ideal I with respect to $\underset{A}{<}$. Then for all $h \in K[X]$,* $\mathrm{nf}_{G_1}(h) = \mathrm{nf}_{G_2}(h)$.

Proof. $\mathrm{nf}_{G_1}(h) - \mathrm{nf}_{G_2}(h) = \mathrm{nf}_{G_1}(h - \mathrm{nf}_{G_2}(h)) = \mathrm{nf}_{G_1}(0) = 0$.
Q.E.D.

Corollary 3 *Let G_1 and G_2 be as in the lemma. Then*

$$\{\mathrm{nf}_{G_1}(h) \ : \ h \in K[X]\} \ = \ \{\mathrm{nf}_{G_2}(h) \ : \ h \in K[X]\} \ .$$

Proof. Let $S = \{\mathrm{nf}_{G_2}(h) \ : \ h \in K[X]\}$, then

$$S \ = \ \{h \ : \ h \in S\} \ = \ \{\mathrm{nf}_{G_1}(h) \ : \ h \in S\} \ \subseteq \ \{\mathrm{nf}_{G_1}(h) \ : \ h \in K[X]\} \ .$$

The other inclusion is symmetric.
Q.E.D.

The most important use of this last corollary is in forming $K[X]/I$. After selecting G_1 a Gröbner basis for I with respect to $\underset{A}{<}$, we can choose $G_2 = \{\mathrm{Head}_A(g) \,:\, g \in G_1\}$, and the corollary assures us that

$$K[X]/I \;=\; \{\mathrm{nf}_{G_1}(h) \,:\, h \in K[X]\} \;=\; \{\mathrm{nf}_{G_2}(h) \,:\, h \in K[X]\}\ .$$

1.1 Minimal Gröbner Bases

A basis F for an ideal I is called a *minimal* basis if for each $f \in F$, $f \notin (F - \{f\})$. Now, suppose that F is a basis for I, but that there exists an $f \in F$ such that $f \in (F - \{f\})$. Then $F - \{f\}$ is also a basis for I. Given a basis F, it is therefore possible to produce a minimal basis $F' \subset F$ by discarding inessential generators.

Lemma 5 *Every monomial ideal $M \subseteq K[X]$ has a unique minimal basis $F = \{f_1, \ldots, f_r\}$ such that each $f_i \in F$ is a power product of* $\mathrm{PP}[X]$.

Proof. Suppose F_1 and F_2 are both power product bases for I and that $a \in F_1 - F_2$. Since $a \in F_1$, $a \in I$. Therefore since F_2 is a Gröbner basis for I there must be a $b \in f_2$ such that b divides a. But now by a similar argument there must be a $c \in F_2$ which divides b and hence also divides a. And since $b \neq a$, c can not be a. This then contradicts the fact that F_1 is a minimal basis.
Q.E.D.

A basis G for an ideal I is called a *minimal* Gröbner basis for I if $\{\mathrm{Head}_A(g) \,:\, g \in G\}$ is a minimal basis for $\mathrm{Head}_A(I)$. Note that a minimal Gröbner basis for I is *not* in general a minimal basis for I. For a Gröbner basis G, let G' be a subset of G such that $\{\mathrm{Head}_A(g) \,:\, g \in G'\}$ is a minimal basis for $\mathrm{Head}_A(I)$. It follows from definition (2) above that G' is a Gröbner basis for I, and hence is a minimal Gröbner basis. As a corollary of the lemma above, if G_1 and G_2 are minimal Gröbner bases for I with respect to $\underset{A}{<}$ and all the polynomials in the two bases are monic, then

$$\{\mathrm{Head}_A(g) \,:\, g \in G_1\} \;=\; \{\mathrm{Head}_A(g) \,:\, g \in G_2\}\ .$$

2 Disjoint Decompositions

Let T be a subset of the polynomial ring $K[X]$. and let $S_1, \ldots, S_r$ be subsets of T. The sets S_i are said to *be a disjoint decomposition of T* if every $p \in T$ can be *uniquely* expressed in the form $p = \sum_{i=1}^{r} p_i$, where $p_i \in S_i$.

The following two important properties of disjunct decompositions can be easily verified.

1. Let $S_1, \ldots, S_k$ be a disjoint decomposition for T, and let $R_1, \ldots, R_m$ be a disjoint decomposition for S_1. Then $S_2, \ldots, S_k, R_1, \ldots, R_m$ is a disjoint decomposition for T.

2. Let $P = \{hf : h \in T\}$, and let $S_1, \ldots, S_k$ be a disjoint decomposition of T. Then the sets $Q_i = \{hf : h \in S_i\}$ form a disjoint decomposition of P.

Example 1: For any ideal $I \subseteq K[X]$, I and $K[X]/I$ form a disjoint decomposition of $K[X]$.

Proof. Let G be the Gröbner basis of I used to form $K[X]/I = \{\mathrm{nf}_G(h)\}$. Since G is a Gröbner basis, each polynomial h has a unique G-normal form, and the decomposition $h = \mathrm{nf}_G(h) + (h - \mathrm{nf}_G(h))$ is unique.

Q.E.D.

Definition: Let I be any ideal of $K[X]$, and $h \in K[X]$. The ideal quotient operation $I : h$ is defined by $I : h \;=\; \{f \in A \;:\; fh \in I\}$. Note that it trivially follows that $(I : g) : h \;=\; I : (gh)$.

Example 2: Given $F = \{f_1, \ldots, f_r\}$ be a basis for I, let

J denote the ideal $(f_1, \ldots, f_{r-1})$,

L denote the ideal $J : f_r$, and

$N = \{hf_r \;:\; h \in K[X]/L\}$, then

J and N form a disjunct decomposition for I.

Proof. Let G be the Gröbner basis for L used to form $N = \{\mathrm{nf}_G(h)f_r \;:\; h \in K[X]\}$. The sets J and N are clearly subsets of I, so we need to show that each polynomial h in I can be uniquely decomposed as $h = h_J + h_N$.

First, we show that a decomposition exists. Every $h \in I$ can be written in the form $h = \sum_{i=1}^{r} a_i f_i$ for $a_i \in K[X]$. Since G is a Gröbner basis for L, we know that $a_r - \mathrm{nf}_G(a_r) \in L$. Now, by definition $L = \{h : hf_r \in J\}$, so $(a_r - \mathrm{nf}_G(a_r))f_r \in J$. This leads to the decomposition $h_J = \sum_{i=1}^{r-1} a_i f_i + (a_r - \mathrm{nf}_G(a_r))f_r \in J$, and $h_N = \mathrm{nf}_G(a_r)f_r$.

Now consider any two decompositions of h: $h = a_1 + \mathrm{nf}_G(b_1)f_r = a_2 + \mathrm{nf}_G(b_2)f_r$, where $a_1, a_2 \in J$.

$$\begin{aligned}(\mathrm{nf}_G(b_1) - \mathrm{nf}_G(b_2))f_r &= a_2 - a_1 \in J \\ \mathrm{nf}_G(b_1) - \mathrm{nf}_G(b_2) &\in L \\ \mathrm{nf}_G(\mathrm{nf}_G(b_1) - \mathrm{nf}_G(b_2)) &= 0 \\ \mathrm{nf}_G(b_1) - \mathrm{nf}_G(b_2) &= 0\end{aligned}$$

Therefore the decomposition is unique.
Q.E.D.

If we apply this technique recursively, we get the following decomposition of an ideal.
Example 3: Let $F = \{f_1, \ldots, f_r\}$ be a basis for I. For each $i \leq r$, let $J_i = (f_1, \ldots, f_{i-1}) : f_i$, and let $P_i = \{hf_i : h \in K[X]/J_i\}$. Then, $P_1, \ldots, P_r$ form a disjoint decomposition of I.

In recap, for any ideal I, $K[X]$ can be decomposed into I and $K[X]/I$. Furthermore, I itself can be decomposed into sets of the form $P_i = \{hf_i : h \in K[X]/J_i\}$, which in turn could be further decomposed if we could decompose $K[X]/J_i$. We therefore need to study sets of the form $K[X]/I$ more closely. We already have one big step in that direction though, because we know that if $M = \mathrm{Head}(I)$, then $K[X]/M = K[X]/I$. And so, we can limit our attention to monomial ideals.

3 Homogeneity and Hilbert Functions

We now will consider one special class of polynomial ideals, and disjoint decompositions, those ideals which are *homogeneous*. For any monomial M, the total-degree $\partial(M)$ is defined by

$$\partial(kx_1^{a_1} \cdots x_n^{a_n}) = \sum_{i=1}^{n} a_i$$

Let f be a polynomial in $K[X]$, then f can be written as a finite sum $f = f_0 + f_1 + \ldots + f_k$, where each f_i is either zero, or a sum of monomials each of which has degree i. In such a decomposition of f, f_i is called the *homogeneous component of f of degree i.*

Definition: f is called a *homogeneous polynomial* if f consists of at most one non-zero homogeneous component.

Definition: S a subset of $K[X]$ is called *homogeneous* if it satisfies the following two properties.

1. $f \in S$ implies that each homogeneous component of f is also in S.
2. $f \in S$ implies that for each $k \in K$, $kf \in S$.

A disjoint decomposition $S_1, \ldots, S_r$ of a homogeneous set T is called a *homogeneous disjoint decomposition* if each S_i is homogeneous.

Of particular importance are homogeneous ideals. The following theorem provides a useful characterization of these ideals.

Theorem 6 *An ideal I is homogeneous if and only if there is a basis for I consisting of homogeneous polynomials.*

For a homogeneous set T, T_d is used to denote the set

$$T_d = \{f \in T : f \text{ is homogeneous of degree } d\} .$$

Note that the sets $T_0, T_1, \ldots$ trivially form a homogeneous disjoint decomposition of T.

[Buchberger 1979] provided an algorithm for forming Gröbner bases. [Giusti 1984] provides a slightly modified version of this algorithm which will calculate a minimal Gröbner basis for a homogeneous ideal. The utilization of Giusti's algorithm is one reason we would like to restict our attention to homogeneous ideals. Another benifit of working with homogeneous ideals is the ability to define the Hilbert function.

The Hilbert function of a homogeneous set T is denoted by $\varphi_T(z)$ and defined by

$$\varphi_T(z) = \text{the dimension of } T_z \text{ as a vector space over } K .$$

Equivalently, for a fixed admissible ordering the Hilbert function may be defined to be the number of degree z power products which occur as the head monomial of a polynomial of T. That is,

$$\varphi_T(z) = |\{p \in \mathrm{PP}[X] : p \in \mathrm{Head}(T_z)\}| .$$

Lemma 7 *Let $S_1, \ldots, S_r$ be a homogeneous disjunct decomposition of T, then $\varphi_T(z) = \sum_{i=1}^{r} \varphi_{S_i}(z)$.*

Proof. This follows directly from the definition of disjunct decomposition and the first definition of the Hilbert function.
Q.E.D.

Our interest in finding a disjoint decomposition for an ideal I is to partition I into primitive elements whose Hilbert function we can easily describe. In particular, the type of elements we want are sets of the form $\{ah : a \in K[u]\}$ where h is a homogeneous polynomial and u is a subset of $X = \{x_1, \ldots, x_n\}$.
Notation: For h a homogeneous polynomial and $u \subseteq X$, let $S(h, u)$ denote the set $\{ah : a \in K[u]\}$.

For a set $S(h, u)$, the Hilbert function of $S(h, u)$ is dependent only on $\deg(h)$ and $|u|$. Counting the number of power products in $\mathrm{Head}(S(h, u))$ we find that if $u = \emptyset$, then

$$\varphi_{S(h,\emptyset)}(z) = \begin{cases} 0 & z \neq \deg(h) \\ 1 & z = \deg(h) \end{cases} ,$$

and for $|u| > 0$,

$$\varphi_{S(h,u)}(z) = \begin{cases} 0 & z < \deg(h) \\ \begin{pmatrix} z - \deg(h) + |u| - 1 \\ |u| - 1 \end{pmatrix} & z \geq \deg(h) \end{cases} .$$

3.1 Homogenizing Affine Ideals

The remainder of this paper builds results which will allow us to obtain a degree bound for polynomials in a Gröbner basis of a homogeneous ideal. But suppose we need to compute a Gröbner basis for an affine ideal. The degree bound in this case is most easily obtained by reducing the affine case to the homogeneous case, as can be done using the following construction provided by [Bayer 1982].

Consider an affine ideal $I \subset A = K[x_1, \ldots, x_n]$, and a basis F for I. Each polynomial $f \in F$, can be written as $f = \sum_{i=0}^{d} f_i$, where f_i is the homogeneous component of f of degree i, and d is the maximum degree of any monomial in f. Now, we can *homogenize* this ideal by the addition of a new variable x_{n+1}. For each $f \in F$, we produce the homogeneous polynomial $\tilde{f} = \sum_{i=0}^{d} f_d x_{n+1}^{d-i}$. Then $\tilde{F} = \{\tilde{f}\}$ is the basis for a homogeneous ideal $\tilde{I} \subset A_{n+1} = K[x_1, \ldots, x_n, x_{n+1}]$. Of course, to be useful we must have a means of returning to the original ring A. We can use the natural homomorphism

$$\sigma(kx_1^{\alpha_1} \ldots x_n^{\alpha_n} x_{n+1}^{\alpha_{n+1}}) \;=\; kx_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Lemma 8 *Let $\tilde{G} = \{g_1, \ldots, g_k\}$ be a basis for $\tilde{I}$. Then, $G = \{\sigma(g_1), \ldots, \sigma(g_k)\}$ is a basis for I.*

Proof.

$(G) \subseteq I$. Let $h \in (G)$, so $h = \sum a_i \sigma(g_i)$ $(a_i \in A)$. Then, $h' = \sum a_i g_i \in \tilde{I}$. But, since $\tilde{F}$ is also a basis for $\tilde{I}$, $h' = \sum b_j \tilde{f}_j$ $(b_j \in A_{n+1})$. But, $h = \sum \sigma(b_j) f_j$, so $h \in I$.

$I \subseteq (G)$. This proof is symmetric to the other inclusion. Let $h \in I$, then $h = \sum b_j f_j$, and $h' = \sum b_j \tilde{f}_j \in \tilde{I}$. Therefore $h' = \sum a_i g_i$ $(a_i \in A_{n+1})$. So, $h = \sum \sigma(a_i)\sigma(g_i)$, and $h \in (G)$.

Q.E.D.

Now that we are interested in finding a Gröbner basis for $\tilde{I}$, we need to settle one more question. What admissible ordering $\underset{\mathrm{B}}{>}$ should we impose on the monomials of A_{n+1}? Our choice is based upon satisfying the upcoming theorem.

Definition: The admissible ordering $\underset{\mathrm{B}}{>}$ is defined as follows. Let $M, N \in A_{n+1}$, then $M \underset{\mathrm{B}}{>} N$ if either

1. $\sigma(M) \underset{\mathrm{A}}{>} \sigma(N)$ or,

2. $\sigma(M) = \sigma(N)$ and $\deg(M) > \deg(N)$.

Lemma 9 *Let $h \in K[x_1, \ldots, x_{n+1}]$ be a homogeneous polynomial. Then $\sigma(Head_B(h)) = Head_A(\sigma(h))$.*

Proof. If h is homogeneous, then every monomial of h has a different σ projection. The ordering $\underset{B}{>}$ is defined such that the monomial whose σ projection is $\underset{A}{>}$-least will appear as $\text{Head}_B(h)$.
Q.E.D.

Theorem 10 *Let $\tilde{G} = \{g_1, \ldots, g_k\}$ be a homogeneous Gröbner basis for $\tilde{I}$ relative to $\underset{B}{>}$. Then, $G = \{\sigma(g_1), \ldots, \sigma(g_k)\}$ is a Gröbner basis for I relative to $\underset{A}{>}$.*

Proof. By the previous lemma, we know that G is a basis for I, so we only need to prove that G is Gröbner. We use the characterization that G is a Gröbner basis if and only if $(\text{Head}_A(G)) = Head_A(I)$. Clearly $\text{Head}_A(G) \subseteq \text{Head}_A(I)$, so we need to show the other inclusion.

Since G is a basis for I, any $h \in I$ can be written as $h = \sum a_i\sigma(g_i)$ with $a_i \in K[x_1, \ldots, x_n]$. Let $h' = \sum a_i g_i$, then $\sigma(h') = h$.

Now $h' \in \tilde{I}$, and $\tilde{I}$ is a homogeneous ideal. Write $h' = \sum_{z=0}^{d} h'_z$ where h'_z is the degree z homogeneous component of h'. Each h'_z is in $\tilde{I}$, so $h^* = \sum_{z=0}^{d} h'_z x_{n+1}^{d-z} \in \tilde{I}$. This polynomial h^* also has the property that $\sigma(h^*) = h$, but moreover h^* is a homogeneous polynomial.

$\tilde{G}$ is a Gröbner basis for $\tilde{I}$, so there is a polynomial $g_i \in \tilde{G}$ such that $\text{Head}_B(g_i)$ divides $\text{Head}_B(h^*)$. But then, $\sigma(\text{Head}_B(g_i)) = \text{Head}_A(\sigma(g_i))$ divides $\sigma(\text{Head}_B(h^*)) = \text{Head}_A(\sigma(h^*)) = \text{Head}_A(h)$.
Q.E.D.

4 Partitioning the Polynomial Space

Definition: A set $P = \{\langle h_1, u_1\rangle, \ldots, \langle h_r, u_r\rangle\}$ *partitions* $T \subseteq K[X]$ if the sets $S(h_i, u_i)$ are a homogeneous disjoint decomposition of T. In particular note that

1. $\{\langle h, u\rangle\}$ partitions $S(h, u)$.

2. $\{\langle 1, X\rangle\}$ partitions $S(1, X) = K[X]$.

3. Let S_1 and S_2 be a disjoint decomposition of T, and let P_1 and P_2 partition S_1 and S_2 respectively, then $P_1 \cup P_2$ partitions T.

4. Let $x_j \in u$, then $\{\langle x_j h, u\rangle, \langle h, u - \{x_j\}\rangle\}$ partitions $S(h, u)$.

5. Let P partition T, $\langle h, u\rangle \in P$, and P' partition $S(h, u)$.
   Then $(P - \langle h, u\rangle) \cup P'$ partitions T.

Definition: For $T \subseteq K[X]$, P is called a *standard partition* of T if

1. P is a partition of T.

2. P is finite.

3. Let $a_P = \min\{\deg(h) : \langle h, u\rangle \in P \ \&\ u \neq \emptyset\}$.
   For every $\langle g, v\rangle \in P$ and degree d such that $a_P \leq d \leq \deg(g)$, P contains a pair $\langle h, u\rangle$ with $deg(h) = d$ and $|u| \geq |v|$.

In particular note that

1. $\{\langle h, u\rangle\}$ is a standard partition of $S(h, u)$.

2. Let S_1 and S_2 be a disjoint decomposition of T, and let P_1 and P_2 partition S_1 and S_2 respectively with $a_{P_1} = a_{P_2}$. Then $P = P_1 \cup P_2$ is a standard partition of T with $a_P = a_{P_1} = a_{P_2}$.

3. Let S_1 and S_2 be a disjoint decomposition of T, and let P_1 and P_2 be standard partitions of S_1 and S_2 respectively with $a_{P_1} < a_{P_2}$. Then, if P_1 contains a pair $\langle g, v\rangle$ with $\deg(g) = a_{P_2} - 1$ and

$$|v| \ \geq \ \max\{|u| : \langle h, u\rangle \in S_1\}$$

   then $P = P_1 \cup P_2$ is a standard partition for T with $a_P = a_{P_1}$.

4. Let P be a standard partition of T, then for any degree d, the set $\{\langle h, u\rangle \in P : \deg(h) \geq d\}$ is a standard partition for some set $T' \subseteq T$.

5. If $P = \{\langle h_1, u_1\rangle, \ldots, \langle h_s, u_s\rangle\}$ is a standard partition for T, then for any homogeneous polynomial c, the set $P' = \{\langle ch_1, u_1\rangle, \ldots, \langle ch_s, u_s\rangle\}$ is a standard partition for $\{ch : h \in T\}$ with $a_{P'} = a_P + \deg(c)$.

There is one special partition which provides a useful function in manipulating standard partitions.

Definition: Let $u = \{x_{j_1}, \ldots, x_{j_m}\} \subseteq X$ Then define the set $E(h, u)$ as

$$E(h,u) \;=\; \{\langle h, \emptyset\rangle\} \cup \{\langle x_{j_i} h, \{x_{j_i}, \ldots, x_{j_m}\}\rangle \;:\; 1 \leq m\} \;.$$

It is easy to verify that $E(h, u)$ is a standard partition of $S(h, u)$.

Lemma 11 *Let Q be a standard partition for T. Then, for any degree $d \geq a_Q$, there exists a standard partition Q_d for the set T with $a_{Q_d} = d$.*

Proof. The proof uses induction on d. For $d = a_Q$, the set Q itself is the standard partition Q_d. Now, assume inductively that we have a standard partition Q_{d-1} for T with $a_{Q_{d-1}} = d-1$. Write Q_{d-1} as $Q_{d-1} = R \cup S$, where $R = \{\langle h, u\rangle \in Q \;:\; \deg(h) = d-1\}$ and $S = \{\langle h, u\rangle \in Q \;:\; \deg(h) \geq d\}$. Then let $R' = \cup_{\langle h,u\rangle \in R} E(h, u)$, and $Q_d = R' \cup S$ is a partition for T_d. It remains to be proven that Q_d is a standard partition. There are two cases to consider:

1. $R = \emptyset$. Then $Q_d = S$, and S is known to have the form of a standard partition.

2. $R \neq \emptyset$. Then $a_{Q_{d-1}} = d-1$, and if S is non-empty then S must contain a pair $\langle h, u\rangle$ with $\deg(h) = d$. Therefore S is either empty, or a standard partition with $a_S = d$. Now, R' consists entirely of pairs $\langle h, u\rangle$ with $\deg(h) = d$, and so R' is trivially a standard partition $a_{R'} = d$. It then follows that $Q_d = R' \cup S$ is also a standard partition with $a_{Q_d} = d$.

Q.E.D.

Corollary 4 *Let S_1 and S_2 be a disjoint decomposition of T, and let P_1 and P_2 be standard partitions of S_1 and S_2 respectively. Then there exists a standard partition P of T with $a_P = \max\{a_{P_1}, a_{P_2}\}$.*

5 Splitting a Monomial Ideal

Let I be an ideal of $K[X] = K[x_1, \ldots, x_n]$ generated by the set of monomials $F = \{f_1, \ldots, f_r\}$. For a given variable x_j, there is a disjoint decomposition of I consisting of I_0 and I_1 where

$$I_0 = I \cap K[X - \{x_j\}]$$

and,

$$I_1 = \{x_j h : h \in K[X] \,\&\, x_j h \in I\} .$$

Clearly, I_0 is an ideal of $K[X - \{x_j\}]$ generated by $F \cap K[X - \{x_j\}]$. It is also easy to verify that I_1 is an ideal of $K[X]$ generated by the set $G = \{g_1, \ldots, g_r\}$, where

$$g_i = \begin{cases} x_j f_i & f_i \in K[X - \{x_j\}] \\ f_i & \text{otherwise} \end{cases} .$$

Comparing the ideal I_1 defined above with $I : x_j$, we find that $I_1 = \{x_j h : h \in I : x_j\}$. Furthermore, this leads us to the fact that $I : x_j$ is generated by $H = \{h_1, \ldots, h_r\}$ where

$$h_i = x_j^{-1} g_i = \begin{cases} f_i & f_i \in K[X - \{x_j\}] \\ x_j^{-1} f_i & \text{otherwise} \end{cases} .$$

Definition: Let $P \cup Q$ be a partition of $T \subseteq K[X]$, and let I be an ideal of $K[X]$. Then P and Q are said to *split* T *relative to* I if

$\langle h, u\rangle \in P$ implies $S(h, u) \subseteq I$ (i.e. $h \in I$), and

$\langle h, u\rangle \in Q$ implies $S(h, u) \cap I = \emptyset$.

In other words, P is a partition of $T \cap I$, and Q is a partition of $T \cap K[X]/I$.

The following two lemmas will provide us with an algorithm to split $K[X]$ relative to a monomial ideal I.

Lemma 12 *Let I be a monomial ideal $g \in \mathrm{PP}[x]$, and let F be a monomial basis for $I : g$. Then, $1 \in F$ implies $S(g, X) \subseteq I$.*

Proof.

$$1 \in F \implies 1 \in I : g \implies g \in I \implies S(g, X) \subseteq I \, .$$

Q.E.D.

Lemma 13 *Let I,g, and F be the same as in the previous lemma, and let $u \subseteq X$. Then $F \cap K[u] = \emptyset$ implies $S(g, u) \cap I = \emptyset$.*

Proof. Assume that $F \cap K[u] = \emptyset$, but that $S(g, u) \cap I$ is non-empty. Then, there exists an $h \in K[u]$ such that $gh \in I$. But this implies that $h \in I : g$, and so there must be an $f_i \in F$ such that Head(h) is a multiple of f_i. But this leads to the contradiction $f_i \in K[u]$.
Q.E.D.

Algorithm for Splitting $S(h, u)$ relative to I

```
SPLIT($h$,$u$,$F$)
  Input : $h \in \mathrm{PP}[X]$
          $u \subseteq X$ is a set of variables
          $F$ a monomial basis for $I : h \subseteq K[X]$
  If $1 \in F$ then return $(P = \{(h, u)\}, Q = \emptyset)$
  If $F \cap \mathrm{PP}[Y] = \emptyset$ then return $(P = \emptyset, Q = \{(h, u)\})$
  Otherwise
    Choose $s \subset u$ a subset of maximum size such that $F \cap K[s] = \emptyset$
    Choose $x_j \in u - s$   [If s=u we would not reach this point.]

    $(P_0, Q_0)$ := SPLIT($h$,$u - \{x_j\}$, $F$)

    For $f_i \in F$, if $f_i \in K[X - \{x_j\}]$ then $f_i' := f_i$
                                        else $f_i' := x_j^{-1} f_i$
    $F' := \{f_i' \; : \; f_i \in F\}$     [$F'$ is a monomial basis for $I : x_j h$.]
    $(P_1, Q_1)$ := SPLIT($x_j h$,$u$, $F'$)
    return $(P = P_0 \cup P_1'$, $Q = Q_0 \cup Q_1)$
End.
```

Lemma 14 *The algorithm terminates.*

Proof. For a set of arguments h, u and F, define the rank of the arguments as $|u| + \sum_{f \in F} \deg(f)$. We now claim if SPLIT is invoked with arguments of rank r, then the two recursive calls (if reached) have arguments of rank $\leq r - 1$. For the first call, this is trivial. For the second call, we must show that there is some $f_i \in F$ such that $f_i \notin \mathrm{PP}[X - \{x_j\}]$. But, this must be true since otherwise we would have $F \cap K[s \cup \{x_j\}] = \emptyset$ contradicting the choose of s, and hence x_j.

If $r = 0$, then F must either be $\{1\}$, or $\emptyset$. In either case, the recursion stops. We can therefore conclude that the depth of recursion is at most r, and hence the algorithm terminates.

Q.E.D.

Corollary 5 *Let F be a monomial basis for the ideal $I : h$. Then SPLIT(h, u, F) produces sets P, and Q which split $S(h, u)$ relative to I. In particular, the set Q is a partition of $S(h, u) \cap K[X]/I$.*

Our main interest in splitting $S(h, u)$ relative to I is the set Q which partitions $S(h, u) \cap K[X]/I$. The algorithm produces P also simply because it is so easy. In the following material however, we will often refer to the set Q as *the* set returned by SPLIT(1,X,F).

Lemma 15 *If the set Q returned by Partition(h, u, F) is non-empty, then Q contains a pair of the form $\langle h, s\rangle$, and for any $\langle g, v\rangle \in Q$, $|s| \geq |v|$.*

Proof. Assume that Q is non-empty, and let $\langle g, v\rangle \in Q$. Then $S(g, v) \subseteq S(h, u)$, and $S(g, v) \cap I = \emptyset$. The only power products in $S(h, u)$ are the set $\{ph : p \in \mathrm{PP}[u]\}$, so $g = ch$ for some $c \in \mathrm{PP}[u]$.

$S(h, v) \cap I$ must also be empty, since otherwise a $p \in K[v]$ such that $ph \in I$ implies $p(ch) \in I$ contradicting the fact that $S(g, v) \cap I$ is empty.

If $v = u$, then the algorithm returns $Q = \{\langle h, u\rangle\}$ satisfying the lemma. Otherwise, the choice of x_j assures that $(S(h, u) \cap K[u - \{x_j\}])/I$ contains $S(h, s)$ where $|s| \geq |u|$. Now, using induction on the depth of recursion, the partition Q_0 contains a pair $\langle h, s\rangle$ where $|s| \geq |u|$. The lemma then follows from the fact that Q_0 is a subset of Q.

Q.E.D.

Lemma 16 *Let I be a monomial ideal of $K[X]$, and let F be the unique minimal power product basis for I. Then, for each $f \in F$, there is a pair $\langle f, u \rangle \in P$.*

Proof. Let f be any element of F. Since $f \in I \cap K[X]$, there is some $\langle h, u \rangle \in P$ such that $f \in S(h, u)$. But, now h is also in I, so $h = bg$ for some $g \in F$. But $f \in S(h, u)$, so we can write f as $f = ah = abg$. We must therefore have $f = h = g$, since otherwise we would contradict the fact that f is a required basis element.
Q.E.D.

Lemma 17 *Let F be a minimal monomial basis for $I \neq K[X]$, and let Q be the set returned by SPLIT$(1, X, F)$. Then for every $f \in F$, Q contains a pair $\langle h, u \rangle$ with $\deg(h) = \deg(f) - 1$.*

Proof. Let P be the other set returned by SPLIT$(1, X, F)$. Let f be any element of F. P is a power product partition, so by the preceding lemma there is a pair $\langle f, v \rangle \in P$. Now, consider how this pair got into P. There must have been a recursive call SPLIT(f, v, F'), where F' is a basis for $I : f$. There also must have been some variable x_j, such that the parent of this recursion was an invocation of SPLIT with parameters SPLIT$(x_j^{-1} f$, v, $F'')$. But then from lemma (15) we find that Q contains a pair of the form $\langle x_j^{-1} f, s \rangle$ satisfying the lemma.
Q.E.D.

Corollary 6 *Let F be a monomial basis for I, and let Q be the set returned by SPLIT$(1, X, F)$. Then if $d = \max\{\deg(h) : \langle h, u \rangle \in Q\}$, I can be generated by the set $\{f \in F : \deg(f) \leq d + 1\}$.*

Lemma 18 *Let Q denote the set returned by SPLIT(h, u, F). Q is a standard partition of $S(h, u) \cap K[X]/(F)$ with $a_Q = \deg(h)$.*

Proof. If Q is either $\emptyset$ or $\{\langle h, u \rangle\}$, then the lemma follows trivially. Otherwise, assume inductively that P_0 and P_1 are standard partitions. P_1 is a standard partition for some set T with $a_T = \deg(h) + 1$. From lemma (15), we know that Q contains a pair $\langle g, v \rangle$ with $\deg(g) = \deg(h)$, and $|v| \geq |s|$ for any pair $\langle f, s \rangle \in Q$. Since the pair $\langle g, v \rangle$ cannot be in P_1, it must be in

P_0, and hence Q is a standard partition with $a_Q = \deg(h)$.
Q.E.D.

Corollary 7 *For any $\langle h, u\rangle \in Q$, $\deg(h) \leq |Q| - 1$.*

Corollary 8 *I can be generated by monomials of degree $\leq |Q|$.*

It follows from the previous remarks that the set Q returned by SPLIT$(1, X, F)$ is a standard partition of $K[X]/(F)$ with $a_Q = 0$. The main result of this section follows immediately from the construction provided by algorithm SLPIT.

Theorem 19 *For any ideal I, there exists a standard partition Q of $K[X]/I$ with $a_Q = 0$.*

Proof. The set $K[X]/I = K[X]/\text{Head}(I)$, and since Head$(I)$ is a monomial ideal the algorithm SPLIT may be used to produce a standard partition.
Q.E.D.

6 Partitioning a Homogeneous Ideal

So far we have seen that for any homogeneous ideal I, there exists an exact partition of $K[X]/I$. But what about I itself? The construction which we presented for partitioning I is only valid for monomial ideals, and even this does not provide a standard partition. The answer is found in the following lemma.

Lemma 20 *Let $F = \{f_1, \ldots, f_r\}$ be a homogeneous basis for an ideal I, then there exists a standard partition P for I with*

$$a_P = \max\{\deg(f_i) \;:\; i \leq r\}.$$

Proof. The proof uses induction on the number of generators r. If $r = 1$, then I is a principle ideal which has the standard partition $P = \{\langle f_1, X\rangle\}$.

Now, assume inductively that the lemma is true for $r - 1$. Recall that if $J = (f_1, \ldots, f_{r-1})$ and $L = J : f_r$, then J and $R = \{hf_r \;:\; f_r \in K[X]/L\}$ form a disjunct decomposition for I. Using the construction provided by

SPLIT, we can form a standard partition Q for $K[X]/L$ with $a_Q = 0$. If $Q = \{\langle h_1, u_1\rangle, \ldots, \langle h_s, u_s\rangle\}$ then it follows that $P_1 = \{\langle f_r h_1, u_1\rangle, \ldots, \langle f_r h_s, u_s\rangle\}$ is a standard partition for R with $a_{P_1} = \deg f_r$.

From the induction hypothesis, there exists a standard partition P_2 of J with $a_{P_2} = \max\{\deg(f_i) : i \leq i - 1\}$. It then follows from corollary (4) that there exists a standard partition P for I with $a_P = \max\{\deg(f_i) : i \leq r\}$. **Q.E.D.**

This result can be slightly improved if we assume that $I \neq \emptyset$. Let $F = \{f_1, \ldots, f_r\}$ be a homogeneous basis for I with $r \geq 2$, and $d = \max\{\deg(f_i) : i = 1, \ldots, r\}$. We have already seen that if we let $J_i = (f_1, \ldots, f_{i-1})$, and $L_i = J_i : f_i$, then the sets $S_i = \{cf_i : c \in K[X]/L_i\}$ form a disjoint partition of I. We also know how to form a standard partition P_i for each S_i in which $a_{P_i} = d$. Now, we could join these into one standard partition P for I as we did in the previous lemma. Instead, keep the set $S_1 = (f_1)$ outside of the standard partition. Then we find that I is the disjoint union of (f_1) and a standard partition P with $a_P = d$. [2]

7 The Exact Partition

Definition: For $T \subseteq K[X]$, Q is called an *exact partition* of T if Q is a standard partition of T and additionally for every degree d, Q contains at most one pair $\langle h, u\rangle$ with $\deg(h) = d$ and $u \neq \emptyset$.

Let Q be an exact partition of T. For $i = 0, \ldots, n + 1$, let

$$b_i = \min\{d \geq a_Q \ : \ \langle h, u\rangle \in Q \ \& \ |u| \geq i \implies \deg(h) < d\} \ .$$

Then for each $i > 0$ and degree d such that $b_{i+1} \leq d < b_i$, there is exactly one pair $\langle h, u\rangle \in Q$ such that $\deg(h) = d$ and $u \neq \emptyset$, and in that pair $|u| = i$. It is a simple consequence of their definition that the b_l's satisfy $b_0 \geq b_1 \geq \cdots \geq b_{n+1} = a_Q$.

Now finally we have reached a type of partition for which we can write the Hilbert function. For $z \geq b_0$, pairs of the form $\langle h, \emptyset\rangle$ do not contribute to the Hilbert function since they all have $\deg(h) < z$. Furthermore, the

[2] The ability to form a standard partition is in many ways similar to the idea of placing an ideal into *generic coordinates*.

Hilbert function of all other $S(h,u)$ sets has reached the point at which it is described by the binomial coefficient

$$\varphi_{S(h,u)}(z) = \binom{z-\deg(h)+|u|-1}{|u|-1}.$$

And so, for $z \geq b_0$, the Hilbert function of a set T which has an exact partition can be expressed in the form:

$$\varphi_T(z) = \sum_{i=1}^{n} \sum_{d=b_{i+1}}^{b_i+1} \binom{z-d+i-1}{i-1}.$$

Using the combinatorial identity

$$\sum_{d=b_{i+1}}^{b_i+1} \binom{z-d+i-1}{i-1} = \binom{z-b_{i+1}+i}{i} - \binom{z-b_i+i}{i},$$

we can write the Hilbert function of T in the form:

$$\begin{aligned}
\varphi_T(z) &= \sum_{i=1}^{n}\left(\binom{z-b_{i+1}+i}{i} - \binom{z-b_i+i}{i}\right) \\
&= \binom{z-b_{n+1}+n}{n} - \binom{z-b_1+1}{1} + \sum_{i=1}^{n-1}\left(\binom{z-b_{i+1}+i}{i} - \binom{z-b_{i+1}+i+1}{i+1}\right) \\
&= \binom{z-b_{n+1}+n}{n} - 1 - \binom{z-b_1}{1} - \sum_{i=1}^{n-1}\binom{z-b_{i+1}+i}{i+1} \\
&= \binom{z-b_{n+1}+n}{n} - 1 - \sum_{i=0}^{n-1}\binom{z-b_{i+1}+i}{i+1} \\
&= \binom{z-b_{n+1}+n}{n} - 1 - \sum_{i=1}^{n}\binom{z-b_i+i-1}{i}
\end{aligned}$$

For P an exact partition of T, we will refer to the constants $b_0, \ldots, b_{n+1}$ as the Macaulay constants of T, in reference to the fact that in [Macaulay 1927] it was first shown that the Hilbert function of $K[X]/I$ can be written in this form.

The following trivial lemma provides a tool by which any standard partition may be transformed into an exact partition.

Lemma 21 *Let Q be a standard partition of T, and let $\langle h,u\rangle, \langle g,v\rangle \in Q$ such that* $\deg(h) = \deg(g)$, *and* $|v| \geq |u| > 0$. *Then for any $x_j \in u$,*

$$Q' = (Q - \{\langle h,u\rangle\}) \cup \{\langle h, u - \{x_j\}\rangle, \langle x_j h, u\rangle\}$$

is also a standard partition of T.

Proof. It must be shown that Q' satisfies the three conditions of the definition of standard partition. The first two conditions follow trivially. The presence of $\langle g,v\rangle \in Q'$ is sufficient to show that the third condition also holds.
Q.E.D.

This lemma provides us with a tool to *shift* pairs away from degrees occupied by other pairs. Consider the following algorithm.

Algorithm for Shifting Pairs in a Standard Partition

```
SHIFT($Q, d, m$)
  Input : $Q$ a standard partition for $T$
          $d$ a degree $\geq 0$
          $m$ a size of a subset of $X$, $1 \leq m \leq n$
  If $\exists\langle h,u\rangle \in Q$ such that $\deg(h) = d$ and $|u| > m$
          then mustkeep := 0
          else mustkeep := 1
  $B$ := $\{\langle h,u\rangle \in Q : \deg(h) = d$ & $|u| = m\}$
  While $|B| > mustkeep$ loop
        Choose $\langle h,u\rangle \in B$ with minimal $|u|$
        Choose $x_j \in u$
        $B$ := $B - \{\langle h,u\rangle\}$
        $Q$ := $(Q - \{\langle h,u\rangle\}) \cup \{\langle h, u - \{x_j\}\rangle, \langle x_j h, u\rangle\}$
  End While loop
  return($Q$)
End.
```

If follows from the previous discussion that the set Q' returned by SHIFT(Q, d, m) is also a standard partition of T. Furthermore, note that

$$|\{\langle h,u\rangle \in Q' : |u| \geq m\} = |\{\langle h,u\rangle \in Q : |u| \geq m\} .$$

Now, using the SHIFT algorithm we can produce an exact partition as follows.

Algorithm for Producing an Exact Partition

```
EXACT($Q$)
  Input : $Q$ a standard partition for $T$
  $Q_{n+1} := Q$
  For $m := n$ down to 1 do
        $Q_m := Q_{m+1}$
        $D := |\{\langle h, u\rangle \in Q_m : |u| \geq m\}|$
        For $d := 0$ to $D - 1$ do
          $Q_m :=$ SHIFT($Q_m, d, m$)
        End For $d$ loop
  End For $m$ loop
  return($Q_1$)
End.
```

Of course this algorithm could be written without the nested loops. It has been written in this way so that termination is obvious. The action of the SHIFT algorithm assures that at all intermediate stages, Q_m remains a standard partition for T. The correctness of the algorithm then follows from the following lemma.

Lemma 22 *For any m and degree d, Q_m contains at most one pair $\langle h, u\rangle$ with* $\deg(h) = d$ *and* $|u| \geq m$.

Proof. Since the claim holds vacuously for $m = n$, we proceed inductively on decreasing values of m. Assume that the claim is true for $m + 1$. The action of SHIFT will then assure that at the conclusion of the For d loop, Q_m contains at most one pair $\langle h, u\rangle$ with $|u| \geq m$ and $\deg(h) = d$ for each degree $d \leq D$. SHIFT also assures that each intermediate set Q_m maintains the fact that $|\{\langle h, u\rangle \in Q_m : |u| \geq m\}|$ remains equal to the constant D. For $d \geq D$ there cannot be a pair $\langle h, u\rangle \in Q$ with $\deg(h) = d$ and $|u| \geq m$ since then the fact that Q is a standard partition would require that $|\{\langle h, u\rangle \in Q_m : |u| \geq m\}| \geq d + 1 \geq D + 1$ which is a contradiction. **Q.E.D.**

The main result of this section follows immediately from the EXACT algorithm.

Theorem 23 *Let T be a subset of $K[X]$ such that there exists Q which is a standard partition of T. Then, there also exists Q' which is an exact partition of T. Furthermore, associated with this exact partition are Macaulay constants $b_0 \geq b_1 \geq \cdots \geq b_{n+1}$, where $b_{n+1} = a_Q$, and $b_0 \geq |Q| - a_Q$, and for $z > b_0$, the Hilbert function of T is described by*

$$\varphi_T(z) = \binom{z - b_{n+1} + n}{n} - 1 - \sum_{i=1}^{n} \binom{z - b_i + i - 1}{i}.$$

Corollary 9 *Let I ba a homogeneous ideal, and let $b_0 \geq b_1 \geq \cdots b_{n+1} = 0$ be the Macaulay constants $K[X]/I$. Then for any admissible ordering $\underset{A}{>}$, the monomial ideal $Head_A(I)$ can be generated by power products of degree $\leq b_0$, and hence a minimal Gröbner basis for I with respect to $\underset{A}{>}$ consists of polynomials whose degrees are also bounded by b_0.*

8 Bounding the Macaulay Constants.

Let $F = \{f_1, \ldots, f_r\}$ be a homogeneous basis for an ideal I. Assume without loss of generality that f_1 has the largest degree $\deg(f_1) = d$. We have shown that there exists a exact partition Q for $K[X]/I$ with $a_Q = 0$. Letting $b_0 \geq b_1 \geq \cdots \geq b_{n+1} = 0$ be the Macaulay constants for $K[X]/I$, we know that for $z \geq b_0$ the Hilbert function of $K[X]/I$ is given by

$$\varphi_{K[x]/I}(z) = \binom{z + n}{n} - 1 - \sum_{i=1}^{n} \binom{z - b_i + i - 1}{i}.$$

It was also shown that I itself has a disjoint decomposition consisting of the principle ideal (f_1) and an exact partition P with $a_P = d$. Letting $a_0 \geq a_1 \geq \cdots \geq a_{n+1} = d$ be the Macaulay constants for the portion of I partitioned by P, for $z \geq a_0$ we can write the Hilbert function of I as

$$\varphi_I(z) = \binom{z - d + n - 1}{n - 1} + \binom{z - d + n}{n} - 1 - \sum_{i=1}^{n} \binom{z - a_i + i - 1}{i}.$$

Now since I and $K[X]/I$ form a disjoint decomposition of $K[X]$, the sum of their Hilbert functions must be equal to the Hilbert function of $K[X]$ which is $\varphi_{K[X]}(z) = \binom{z+n-1}{n-1}$. Therefore, for $z \geq \max\{a_0, b_0\}$ we find that

$$\binom{z+n-1}{n-1} = \binom{z-d+n-1}{n-1} + \binom{z-d+n}{n} + \binom{z+n}{n} \\ -2 - \sum_{i=1}^{n} \left[\binom{z-a_i+i-1}{i} + \binom{z-b_i+i-1}{i} \right].$$

The backwards difference operator ∇ is defined for any function $F(z)$ by: $\nabla F(z) = F(z) - F(z-1)$, and $\nabla^j F(z) = \nabla(\nabla^{j-1} F(z))$. Using the identity $\binom{z+k}{n} - \binom{(z-1)+k}{n} = \binom{z+k-1}{n-1}$ we induce that $\nabla^j \binom{z+k}{n} = \binom{z+k-j}{n-j}$.

Now if $F_1(z) = F_2(z)$ for $z > k$, then clearly $\nabla F_1(z) = \nabla F_2(z)$ for $z > k+1$. We can therefore apply the backwards difference operator to the equation above and find that for sufficiently large z, for each $j = 0, \ldots, n-1$ we get an equation:

$$\binom{z+n-j-1}{n-j-1} = \binom{z-d+n-j-1}{n-j-1} + \binom{z-d+n-j}{n-j} + \binom{z+n}{n} \\ -2 - \sum_{i=j+1}^{n} \left[\binom{z-a_i+i-j-1}{i-j} + \binom{z-b_i+i-j-1}{i-j} \right].$$

Now, each side of these equations is a polynomial in z, so they must agree for each power of z. In particular, they must have the same constant term. Noting that the constant term of $\binom{z+k}{n}$ is given by

$$\binom{0+k}{n} = \begin{cases} \binom{k}{n} & k \geq 0 \\ (-1)^n \binom{k+n-1}{n} & k < 0 \end{cases}$$

leads to the equations

$$\begin{aligned} 1 &= (-1)^{n-j-1}\binom{d-1}{n-j-1}+(-1)^{n-j}\binom{d-1}{n-j} \\ &\quad -1-\sum_{i=j+1}^{n}(-1)^{i-j}\left[\binom{a_i}{i-j}+\binom{b_i}{i-j}\right] . \end{aligned}$$

At $j = n-1$, this yield

$$1-\binom{d-1}{1}-1+a_n+b_n=1 .$$

So $a_n + b_n = d$. But we already have the conditions $a_n \geq d$, and $b_n \geq 0$. Therefore, it must be the case that $a_n = d$. Substituting these values the series of equations becomes:

$$2(-1)^{n-j-1}\binom{d-1}{n-j-1}-1-\sum_{i=j+1}^{n-1}(-1)^{i-j}\left[\binom{a_i}{i-j}+\binom{b_i}{i-j}\right]=1 .$$

Let c_{j+1} denote the sum $a_{j+1} + b_{j+1}$. Solving for this expression yields

$$c_{j+1} = 2+2(-1)^{n-j}\binom{d-1}{n-j-1}+\sum_{i=j+2}^{n-1}(-1)^{i-j}\left[\binom{a_i}{i-j}+\binom{b_i}{i-j}\right] .$$

At this point, we note that the sum on the right is vacuous for $j = n-2$ we can conclude that $c_{n-1} = 2+2(d-1) = 2d$. And since,

$$\binom{a_{i+1}}{k}+\binom{b_{i+1}}{k} \leq \binom{c_{i+1}}{k} , \qquad (1)$$

is true for all i, for $j = n-3$ we get,

$$c_{n-2} \leq 2-2\binom{d-1}{2}+\binom{2d}{2} = d^2+2d .$$

The expression for the remaining c_{j+1}'s contains the term

$$2+(-1)^{n-j}\left[2\binom{d-1}{n-j-1}-\binom{a_{n-1}}{n-j-1}-\binom{m_{n-1}}{n-j-1}\right] .$$

The magnitude of this combination is bounded by $\binom{c_{n-1}}{n-j-1}$, so we obtain the inequalities

$$c_{j+1} \leq \binom{c_{n-1}}{n-j-1} + \sum_{i=j+2}^{n-2} (-1)^{i-j} \left[\binom{a_i}{i-j} + \binom{b_i}{i-j} \right] .$$

Now, noting that the term in the sum for $i = j+3$ has a negative sign, we may discard this term, and make all other terms positive to obtain the simpler inequalities:

$$\begin{aligned} c_{j+1} &\leq \binom{c_{n-1}}{n-j-1} + \left[\binom{a_{j+2}}{2} + \binom{b_{j+2}}{2} \right] + \sum_{i=j+4}^{n-2} \left[\binom{a_i}{i-j} + \binom{b_i}{i-j} \right] \\ &\leq \binom{c_{j+2}}{2} + \sum_{i=j+4}^{n-1} \binom{c_i}{i-j} . \end{aligned}$$

Or, repairing the subscripts,

$$c_j \leq \binom{c_{j+1}}{2} + \sum_{i=j+3}^{n-1} \binom{c_i}{i-j+1} .$$

We now claim that for $j \leq n-2$, $c_j \leq 2(\frac{d^2}{2} + d)^{2^{n-j-1}}$.
Proof. We have already determined that $c_{n-2} \leq d^2 + 2d$, satisfying this claim. Now, assume inductively that c_i has the indicated form for $j < i \leq n-2$.
For $i \geq j+3$ the inequality $2^{i-j-1} \geq i-j+1$ can be used to see that $(2^{n-i-1})(i-j+1) \leq 2^{n-j-2}$. Therefore,

$$\binom{c_i}{i-j+1} \leq \frac{c_i^{i-j+1}}{(i-j+1)!} \leq c_{j+1}\frac{2^{i-j}}{(i-j+1)!} .$$

And so,

$$\begin{aligned} c_j &\leq \binom{c_{j+1}}{2} + \sum_{i=j+3}^{n-1} \binom{c_i}{i-j+1} \\ &\leq \frac{c_{j+1}^2 - c_{j+1}}{2} + \sum_{i=j+3}^{n-1} c_{j+1}\frac{2^{i-j}}{(i-j+1)!} \end{aligned}$$

$$\begin{aligned} &\leq \frac{c_{j+1}^2}{2} - c_{j+1}\left[1/2 - \sum_{i=j+3}^{n-1} \frac{2^{i-j}}{(i-j+1)!}\right] \\ &\leq \frac{c_{j+1}^2}{2} = 2(\frac{d^2}{2}+d)^{2^{n-j-1}} . \end{aligned}$$

Q.E.D.

From this then we can conclude that the Macaulay constants a_1 and b_1 are each less than $c_1 \leq 2(\frac{d^2}{2}+d)^{2^{n-2}}$. But what about the constants a_0 and b_0 which did not appear explicitly in the Hilbert function. Notice that the equality $\varphi_I(z) + \varphi_{K[X]/I}(z) = \varphi_{K[X]}$ which was claimed valid for $z > \max\{a_0, b_0\}$ actually holds for $z \geq \max\{a_1, b_1\}$. If either partition contained a set $S(h, \emptyset)$ with $\deg(h) = d_0 > \max\{a_1, b_1\}$, then the this would increase the Hilbert function $\varphi_I(z) + \varphi_{K[X]/I}(z)$ at degree $z = d_0$ destroying the equality which must exist at every degree. Therefore, both a_0 and b_0 must be $\leq \max\{a_1, b_1\}$.

In conclusion, if I is a homogeneous ideal generated by polynomials of degree $\leq d$, Then the Macaulay constant b_0 of $K[X]/I$ must satisfy the bound given above for c_1. This constant b_1 in turn provides an upper bound on the degree power products which are required to generate Head(I), and since these power products appear as the head terms of polynomials in a Gröbner basis for I, the degree of required Gröbner basis polynomials is also bounded by the constant c_1.

References

[Bachmair and Buchberger 1980] L. Bachmair and Bruno Buchberger, *A simplified proof of the characterization theorem for Gröbner-bases*, **SIGSAM 14**, 29-34.

[Bayer 1982] David Bayer, *The Division Algorithm and the Hilbert Scheme* **Ph.D. thesis, Harvard University 1982.**

[Bayer 1985] David Bayer, *An Introduction to the Division Algorithm*, informal notes.

[Bayer and Stillman 1987] David Bayer and Michael Stillman, *A criterion for detecting m-regularity*, **Inventiones mathematicae 87**, 1-11.

[Buchberger 1979] Bruno Buchberger, *A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Basis*, **SYMSAC 1979**, 3-20.

[Buchberger 1985] Bruno Buchberger, *Gröbner basis: An algorithmic method in polynomial ideal theory*, in chapter 6 of **Multidimensional Systems Theory**, (editor, N. K. Bose), D.Reidel Publishing Company, 184-229.

[Dubé, Mishra and Yap 1986] T. Dubé, B. Mishra and C. Yap, *Normal form algorithms and admissible orderings in Gröbner bases* **in preparation.**

[Giusti 1984] M. Giusti, *Some Effectivity Problems in Polynomial Ideal Theory*, *Lecture Notes in Computer Science 174*, 1984,159-171.

[Lazard 1984] D. Lazard, *Gröbner basis, Gaussian elimination and resolution of systems of algebraic equations.*, *Lecture Notes in Computer Science 174*, 1984, 146-156.

[Macaulay 1927] F.S. Macaulay, *Some Properties of Enumeration in the Theory of Modular Systems*, **Proceedings of the London Mathematical Society 26**, 1927, 531-555.

[Mishra and Yap 1986] B. Mishra and C.Yap, *Notes on Gröbner Basis*, **in preparation.**

[Möller and Mora 1984] H. Michael Möller and Ferdinando Mora, *Upper and Lower Bounds for the Degree of Groebner Bases*, *Lecture Notes in Computer Science 174*, 1984,172-183.

[Robbiano 1985] L. Robbiano, *Term Orderings on the Polynomial Ring*, 1985, 513-517.

[Stanley 1978] Richard P. Stanley, *Hilbert Functions of Graded Algebras*, **Advances in Mathematics 18**, 1978,57-83.

[Zariski and Samuel 1960] Oscar Zariski and Pierre Samuel, *Commutative Algebra, Volume II*, **Springer-Verlag 1960.**

NYU COMPSCI TR-341 c.2
Dube, Thomas W
The structure of polynomial
ideals and Grobner bases.